POLICY 078
PERSONAL DATA PROCESSED BY STUDENTS

If you have a disability which makes reading this document or navigating our website difficult and you would like to receive information in an alternative format, please contact: anddegree@acm.ac.uk

POLICY 078: PERSONAL DATA PROCESSED BY STUDENTS

1. PURPOSE

1.1 This guidance is intended for students undertaking research or other work involving information about living, identifiable individuals as part of their programme of study at ACM.

2. POLICY DETAILS

2.1 The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 protect the rights of individuals when you process personal data about them, including obtaining, holding and destroying it.

2.2 The definition of personal data is highly complex. For day-to-day purposes, it is best to assume that all information about a living, identifiable individual is personal data. This includes any expression of opinion by or about the individual.

2.3 Students use personal data for two main reasons:

1. To maintain a personal life, for example to communicate with family and friends.
2. To pursue a course of study with the university, for example to research and write an essay, report or thesis.

2.4 Students may use many different methods to process personal data, such as maintaining an email account, a computer database, or using social media accounts.

3. POLICY SCOPE

3.1 Only in very limited and specific circumstances is ACM responsible for personal data processed by students (see 3.11 to 3.15), and only in these specific circumstances does it become the data controller for that data. A data controller is the person who determines the purposes for which, and the manner in which, any personal data is or is not to be processed. Therefore, ACM is only responsible for the personal data processed by its students when the students process data for the university's purposes. In all other circumstances students process data for their own purposes and not ACM's.

Personal, domestic and household purposes

3.2 Personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, falls outside the scope of UK and EU GDPR (Recital 18). This means that where personal data is used for such things as writing to friends and family or taking pictures for your own enjoyment, students are not subject to the GDPR even if they are using ACM email accounts.

3.3 ACM is not the data controller for personal data processed by students in the course of their personal life, as ACM does not determine the purpose of the processing. The fact that students may choose to use their ACM-provided email account to pursue their personal life does not make ACM responsible for the processing of personal data for that purpose.

3.4 ACM does not determine the purpose so cannot be the data controller. Students are the data controller and may claim the so-called 'purely personal or household activity' exemption. Use of this exemption has the effect that data protection laws do not apply to the processing activity.

Use of personal data in pursuit of a course of study

3.5 Where a student processes personal data in order to pursue a course of study with ACM, ACM is not the data controller for the personal data processed by that student.

3.6 Students undertake a course of study with ACM for their own personal purposes, most obviously to obtain a qualification. Students are not employees or agents of ACM and neither do they act on behalf of ACM. Students decide what work they will do, the way in which they will do it and what they will include in their final submission. They must make these decisions themselves in order to prove that they are capable of Bachelors degree-level or Masters degree-level work. They do this work on behalf of themselves and not ACM. Thus, ACM cannot be the data controller for the personal data processed by students in the course of their studies.

3.7 However, the student will still be bound by the ACM's policy and procedures due to their student contract with ACM. This means that when students are processing personal data as part of their work to pursue a course of study, ACM's Data Access and Protection Policy (and Research Ethics Policy) applies to them, and they will be required to ensure that their work complies with the data protection principles.

3.8 This contractual duty to comply with the ACM's Data Protection Policy extends to all work related to the course of study, even if the student contract has expired, such as a promise to inform research participants of results after the dissertation has been submitted and approved.

3.9 If a student subsequently uses the work generated during their course of study as the basis for a post as academic researcher at ACM, then ACM is the data controller for this follow-on work.

3.10 Students using personal data in their dissertation research must complete the ACM Research Ethics Form and a Participant Consent Form.

Personal data submitted to ACM as part of an assessment

3.11 When a student submits a piece of work containing personal data to ACM for assessment (e.g. a dissertation or thesis), ACM and the student become joint data controllers for the personal data contained within the submitted piece of work from the point at which it is submitted.

3.12 Once the work has been submitted, ACM is jointly responsible for the personal data within the document. For example, the member of ACM staff who marks the work is processing the personal data contained within it (by reading it) for the purpose of determining what grade ACM should award the student. This is ACM's purpose. The legal basis for ACM using this data falls under 'Public Task' in Article 6 of the UK GDPR.

3.13 If the work is then transferred to the ACM library to be put on reference (for example if it is a PhD thesis), ACM is responsible for any processing of the personal data associated with the document being placed on reference. This is because providing a reference service is a university purpose.

University-led postgraduate research groups

3.14 In cases where a research student processes personal data whilst working on a project led by a university research group, the university is the data controller for personal data processed by the student. This is because the student processes personal data for the purposes laid down by the project, the remit of which has been decided by the university (or the university-employed project leader), not the student. In this scenario, the student is an agent of the university. This is the case whether the student is funded by the research project or whether the student is self-funding. The legal basis for ACM using this data falls under 'Public Task' in Article 6 of the UK GDPR.

University-sponsored studies

3.15 In cases where a university is a sponsor or co-sponsor of a study, and where a research student processes personal data in order to pursue a course of study in

connection with that (co-)sponsored study, the university is the data controller. The legal basis for ACM using this data falls under 'Public Task' in Article 6 of the UK GDPR.

4. GOOD PRACTICE IN USING PERSONAL DATA RESPONSIBLY

4.1 The following steps are examples of good practice in using personal data responsibly:

1. Before you start your research, consider carefully what personal data you need to collect for your dissertation or thesis and obtain the consent of your supervisor.
2. Obtain ethical consent from the data subject. For research this will usually be in writing. Discuss with your supervisor any concerns about obtaining consent **before** collecting personal data. Be aware that collecting personal data before consent is obtained may be treated as academic misconduct.
3. Give a clear explanation of what you are going to do with the data to the people participating in your research.
4. Do not collect or keep data that is not necessary for your research. Anonymise data where possible by removing names and other identifying information.
5. Ensure that all personal data, especially opinions, is recorded accurately.
6. Respect reasonable requests to update or delete data you have collected.
7. Store personal data securely. Password protection and restricting access to drives is good practice. If you are using information that is already public knowledge such as the names of Grammy award winners, you will not need to take any security measures. However if you are recording less public information, you **must** ensure that the information is secure.
8. Do not disclose personal data to anyone except the individual concerned.
9. Securely destroy personal data when it is no longer necessary for your research. Consult the Assessment Regulations to confirm how long you will need to retain research data for (usually one calendar year).
10. Be aware of required safeguards for international transfers of personal data outside of the UK.

5. RELATED POLICIES

5.1 Internal

- Data Access and Protection Policy
- Research Ethics Policy

5.2 External

- Data Protection Act 2018 (DPA 2018)
- UK General Data Protection Regulation (GDPR)

6. POLICY OWNER

This Policy is under the responsibility of the Academic Board. The responsible committee will ensure the cyclical review of this Policy is carried out under ACM's Quality Assurance Framework.

The Academic Board delegates operational responsibility of this Policy to:

- Quality Assurance and Enhancement Manager
- ACM Research Ethics Chair
- ACM Research Supervisors

7. DOCUMENT HISTORY AND NEXT REVIEW

Version	1.0
Approved by	Academic Board
Approved on	20 March 2025
Review due	August 2026